Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:
VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:
Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

    a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.

    b. Records Officer is responsible for supplying records retention and deletion schedules.

    c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

    d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

    e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)
Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form
Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name: Region 3>VHA>VISN 7> Charleston VAMC>LAN

OMB Unique System / Application / Program Identifier   (AKA: UPID #):   029-00-02-00-01-1120-00

Description of System/ Application/ Program: The Charleston, SC VAMC LAN supports mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health 0Administration. Applications and devices within the LAN support numerous areas, including medical imaging, supply management, decision support, medical research, and education. The LAN is comprised of workstations, servers, printers and other equipment which include devices such as routers, hubs, switches, and firewalls that support communications to extended LAN locations such as community based outpatient clinics (CBOC's). The LAN system also includes subsystem components such as tape drives, disk drives, uninterruptible power supplies (UPS), network area storage (NAS), and storage access networks (SAN). Within this plan each facility will document their own physical description of their LAN system including local and extended LAN locations, its components and subsystems. Access to the LAN system is via wired or wireless devices using TCP/IP and other protocols operating on a variety of operating systems including UNIX, Linux, and Windows-family operating systems. Devices which access the LAN system include government furnished equipment (GFE) such as: personal computers, thin clients, various models of "dumb" terminals, portable computing devices and medical device systems. Clients primarily connect over the TCP/IP network using terminal emulation software and remote procedure call (RPC) broker to VistA or other network resources such as file, print or application servers and telephone systems.

Facility Name:

Title:	Name:	Phone:	Email:
Privacy Officer:	Sandra Lombardi	843-789-7767	sandra.lombardi@va.gov
Information Security Officer:	Jimmy Morrison	843-789-7036	jimmy.morrison@va.gov
System Owner/ Chief Information Officer:	David Olivera	843-789-7400	david.olivera@va.gov
Information Owner:	David Olivera	843-789-7400	david.olivera@va.gov
Other Titles: LAN System Manager	Ronald Wilkinson	843-789-6585	ronald.wilkinson@va.gov
Person Completing Document:	Sandra Lombardi	843-789-7767	sandra.lombardi@va.gov

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)   12/2008

Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, Sections 501(b) and 304.

What is the expected number of individuals that will have their PII stored in this system: 100000-300000

Identify what stage the System / Application / Program is at: Operations/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or
Development stage), or the approximate number of years the system/application/program has
been in operation.   17 years

Is there an authorized change control process which documents any changes to existing
applications or systems?   Yes

If No, please explain:

Has a PIA been completed within the last three years?   Yes

Date of Report (MM/YYYY):   2/23/2011

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

☐ Have any changes been made to the system since the last PIA?

☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?

☐ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☑ Does this system/application/program collect, store or disseminate PII/PHI data?

☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system, please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

For each applicable System(s) of Records, list:

    1. All System of Record Identifier(s) (number):

    2. Name of the System of Records:

    3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Does the System of Records Notice require modification or updating?

Is PII collected by paper methods?

Is PII collected by verbal methods?

Is PII collected by automated methods?

Is a Privacy notice provided?

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

24VA19

Patient Medical Records—VA

http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm

Yes

No

(Please Select Yes/No)

Yes

Yes

Yes

Yes

Yes

Yes

Yes

Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	N/A			
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	Electronic/File Transfer	Data necessary for Health Care	Verbal & Written	Verbal & Written
Criminal Record Information				
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	N/A			
Other (Explain)				

Item 15 is N/A no selection available

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	No			
Family Relation (spouse, children, parents, grandparents, etc)	No			

Service Information	No		
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory
Criminal Record Information	No		
Guardian Information	No		
Education Information	No		
Benefit Information	No		
Other (Explain)			
Other (Explain)			
Other (Explain)			

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	N/A	No		N/A	
Other Veteran Organization	N/A	No		N/A	
Other Federal Government Agency	N/A	No		N/A	
State Government Agency	N/A	No		N/A	
Local Government Agency	N/A	No		N/A	
Research Entity	N/A	No		N/A	
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	
Per responses in Tab 4, does the system gather information from an individual?	No

If information is gathered from an individual, is the information provided:
☐ Through a Written Request
☐ Submitted in Person
☐ Online via Electronic Form

Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	No

if yes, please check all that apply:
☐ Drug/Alcohol Counseling   ☐ Mental Health   ☐ HIV
☐ Research   ☐ Sickle Cell   ☐ Other (Please Explain)

Describe process for authorizing access to this data.

Answer:

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or
any party if disclosed to the public?   No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: The LAN stores information extracts from VistA, DSS and other individual systems. The LAN itself
is not an information system designed or used to perform collection of information from the
public. Personally identifiable information (PII) is stored on the LAN, but the LAN itself
does not collect PII for its own purpose (e.g., extracts from VistA that contain PII may be stored
on the LAN for specific uses by authorized personnel).

How is data checked for completeness?

Answer: Collections of data that use the LAN for storage have their own System of Records Notice if applicable (e.g., Decision Support System data is
included in System of Records 121VA19 and VistA data falls under 79VA19). Additionally, systems that collect PII and store it on the LAN have their
own PIAs, detailing the types of information collected. That information is not repeated here as the LAN does not collect the information. It is solely
used as storage for the systems that do collect the information.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Collections of data that use the LAN for storage have their own System of Records Notice if applicable (e.g., Decision Support System data is
included in System of Records 121VA19 and VistA data falls under 79VA19). Additionally, systems that collect PII and store it on the LAN have their
own PIAs, detailing the types of information collected. That information is not repeated here as the LAN does not collect the information. It is solely
used as storage for the systems that do collect the information.

How is new data verified for relevance, authenticity and accuracy?

Answer: Collections of data that use the LAN for storage have their own System of Records Notice if applicable (e.g., Decision Support System data is
included in System of Records 121VA19 and VistA data falls under 79VA19). Additionally, systems that collect PII and store it on the LAN have their
own PIAs, detailing the types of information collected. That information is not repeated here as the LAN does not collect the information. It is solely
used as storage for the systems that do collect the information.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Data is maintained in accordance with VA Directive 6300, http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FType=2, VA Handbook 6300.1, http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FType=2, and VHA Records Control Schedule 10-1, http://vaww1.va.gov/vhapublications/rcs10/rcs10-1.pdf. The final, consolidated, electronic version of a Patient Medical Record, including information migrated from interim electronic information systems, electronic medical equipment, or information entered directly into the patient medical record information system is destroyed/deleted 75 years after the last episode of patient care, in accordance with RCS 10-1, XLIII, 2.b., Electronic Final Version of Health Record.

Explain why the information is needed for the indicated retention period?

Answer: Veterans Health Administration (VHA) Records Control Schedule (RCS) 10-1 is the main authority for the retention disposition of VHA records. It provides a brief description of the records and states the retention and disposition requirements. It also provides the National Archives and Records Administration NARA (NARA) disposition authorities or the General Records Schedules (GRS) authorities, whichever is appropriate for the records.

What are the procedures for eliminating data at the end of the retention period?

Answer: Data is stored in accordance with VA Records Control Schedule 10-1. When no longer needed, VA sensitive information is destroyed by a method rendering it unreadable, undecipherable, and irretrievable as outlined in VA's current electronic sanitization procedures. (VA HB 6500, paragraph 6. b.(4)(b)16.d)

Where are these procedures documented?

Answer: VA Directive 6300, http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FType=2, VA Handbook 6300.1, http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FType=2, and VHA Records Control Schedule 10-1, http://vaww1.va.gov/vhapublications/rcs10/rcs10-1.pdf.

How are data retention procedures enforced?

Answer: VA Records Control Schedule 10-1 (page 8): Records Management Responsibilities The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities.
Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)	Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?   No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access?	Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: Security control assessments are conducted as part of certification and accreditation efforts. Controls that are not implemented become part of a Plan of Action and Milestones and are tracked until mitigated. An intrusion prevention system monitors network traffic in real time. Audit logs are examined regularly for possible incidents.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

☑ Air Conditioning Failure

☑ Chemical/Biological Contamination

☐ Blackmail

☑ Bomb Threats

☐ Burglary/Break In/Robbery

☐ Cold/Frost/Snow

☑ Communications Loss

☑ Computer Intrusion

☑ Computer Misuse

☑ Data Destruction

☑ Data Disclosure

☑ Data Integrity Loss

☐ Denial of Service Attacks

☑ Earthquakes

☐ Eavesdropping/Interception

☑ Errors (Configuration and Data Entry)

☑ Fire (False Alarm, Major, and Minor)

☑ Flooding/Water Damage

☑ Fraud/Embezzlement

☑ Hardware Failure

☑ Identity Theft

☐ Malicious Code

☑ Power Loss

☑ Sabotage/Terrorism

☑ Storms/Hurricanes

☑ Substance Abuse

☐ Theft of Assets

☑ Theft of Data

☑ Vandalism/Rioting

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

☑ Access Control

☑ Audit and Accountability

☑ Awareness and Training

☑ Certification and Accreditation Security Assessments

☑ Configuration Management

☑ Contingency Planning

☑ Identification and Authentication

☑ Incident Response

☑ Media Protection

☑ Personnel Security

☑ Physical and Environmental Protection

☑ Risk Management

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: The LAN system is inspected under SCA(Security Controls Assessment) every three years and annually by local inspection using the security controls found in NIST 800-53 Rev3 and VA Directive/Handbook 6500 to mitigate compromise of the information stored on the sytem.

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.

| Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon | ☑ | The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. |
| | ☐ | The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. |

the system or organization?   (Choose One)

The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performace Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitelment Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Vertified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Which of these are sub-components of your system?

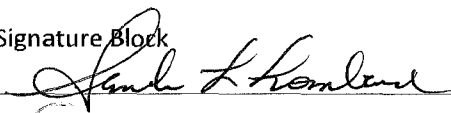|		
1184 Web	ENDSOFT	RAFT
	Enterprise Terminology Server &	RALS
A4P	VHA Enterprise Terminology	
	Services	

(FY 2011) PIA: Final Signatures

Facility Name: Region 3>VHA>VISN 7> Charleston VAMC>LAN
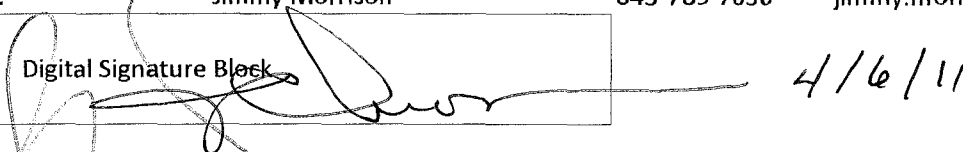
Title	Name	Phone	Email
Privacy Officer:	Sandra Lombardi	843-789-7767	sandra.lombardi@va.gov

Digital Signature Block

Information Security Officer:	Jimmy Morrison	843-789-7036	jimmy.morrison@va.gov

Digital Signature Block

4/6/11

System Owner/ Chief Information Officer:	David Olivera	843-789-7400	david.olivera@va.gov

Digital Signature Block

Information Owner:	David Olivera	843-789-7400	david.olivera@va.gov

Digital Signature Block

Other Titles: LAN System Manager	Ronald Wilkinson	843-789-6585	ronald.wilkinson@va.gov

Digital Signature Block

Date of Report: 4/6/11
OMB Unique Project Identifier   029-00-02-00-01-1120-00
                                                              Region 3>VHA>VISN 7> Charleston
Project Name   VAMC>LAN